Борзенкова С.Ю.
Borzenkova S.U.

АСПЕКТЫ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ» С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНЫХ СРЕДСТВ КОМПЬЮТЕРНОЙ ТЕХНИКИ

ASPECTS OF STUDYING OF DISCIPLINE «CRYPTOGRAPHIC PROTECTION OF THE INFORMATION» WITH USE OF SOFTWARE OF COMPUTER TECHNICS

tehnol_sb@tsu.tula.ru
ГОУ ВПО "Тульский государственный университет"
г. Тула

Рассматривается процесс реализации защиты информации с помощью криптографического алгоритма метода перестановки с использованием компьютерных технологий. Программа, разработанная для реализации криптографического метода перестановки, предназначена для практических заданий при изучении дисциплины «Криптографическая защита информации».

Process of realization of protection of the information by means of cryptographic algorithm of a method of permutation with use of computer technologies is considered. The program developed for realization of a cryptographic method of permutation, is intended for practical tasks at discipline studying «Cryptographic protection of the information».

Широкое распространение компьютерной техники за последние годы и связанный с этим резкий рост объемов информации (в том числе и конфиденциальной), передаваемой по открытым каналам диктуют необходимость применения надежных средств защиты информации.

Построение систем защиты информации, также как и информационной безопасности организации основывается на принципах системного подхода, который предполагает оптимальную пропорцию между организационными, программными, правовыми и физическими методами защиты, применимых на любом этапе цикла обработки информации.

Конкретные реализации систем защиты, которые могут существенное отличаться друг от друга из-за различия методов и алгоритмов, должны обеспечивать задачи конфиденциальность и целостность информации. Успешное решение перечисленных задач возможно как за счет использования организационно-технических мероприятий, так и с помощью криптографической защиты информации.

Криптографическая защита в большинстве случаев является более эффективной и дешевой. Конфиденциальность информации при этом обеспечивается шифрованием передаваемых документов.

Программная реализация криптографического закрытия данных должна обеспечивать выполнение следующих требований:

- дешифровать сообщение можно только при наличии ключа;

- знание алгоритма шифрования не должно влиять на надежность защиты;
- любой ключ из множества возможных ключей должен обеспечивать надежную защиту;
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Современный специалист по защите информации должен иметь представление о методах и алгоритмах защиты от несанкционированного блокирования, доступа, копирования и изменения информации, которые реализуются методами криптографии. Одной из дисциплин, базирующихся на изучении методов и алгоритмов современной криптографии, и которую изучают студенты, обучающиеся на специальности «Организация и технология защиты информации», является дисциплина «Криптографическая защита информации».

Дисциплина «Криптографическая защита информации» включает как теоретические занятия, так и практические. Практические занятия обеспечивают основную практическую подготовку специалиста в области защиты информации при изучении различных криптографических алгоритмов защиты информации.

Программа, разработанная для реализации криптографического метода перестановки, выполнена на языке программирования Турбо Паскаль.

Для того чтобы пользователь мог успешно работать с программой шифрования и дешифрования необходимо наличие программ с расширение .PAS и файлов с расширением .TXT (для вывода информации в файл).

Процесс шифрования включает следующие действия пользователя:

- установить выходные и входные файлы (файлы с расширением .TXT) на жесткий диск;
- запустить файл с программой шифрования (файл с расширением .PAS);
- ввести ключевое слово;
- ввести сообщение. В данной программе вводится ограничение: все буквы должны вводиться либо прописными, либо заглавными.
- открыть выходной файл, который автоматически изменяется при вводе нового сообщения и записывается на жестком диске);

Алгоритм процесса шифрования представлен в левой части рисунка.

При нормальной работе программы пользователь увидит поэтапную последовательность процесса шифрования.

Процесс дешифрования выполняется по следующему алгоритму:

- в входной файл (файл с расширением .TXT) записать ключ и следующей строкой зашифрованное сообщение;
- запустить программу дешифрования (файл с расширением .PAS);
- после выполнения программы пользователь должен открыть выходной файл, где будет записано расшифрованное сообщение.

Алгоритм процесса дешифрования представлен в правой части рисунка.

Данная программа предназначена для использования выполнения практического задания по изучению криптографического метода перестановки. В программе предусмотрены изменения количества символов, как в ключевом слове, так и в исходном сообщении.

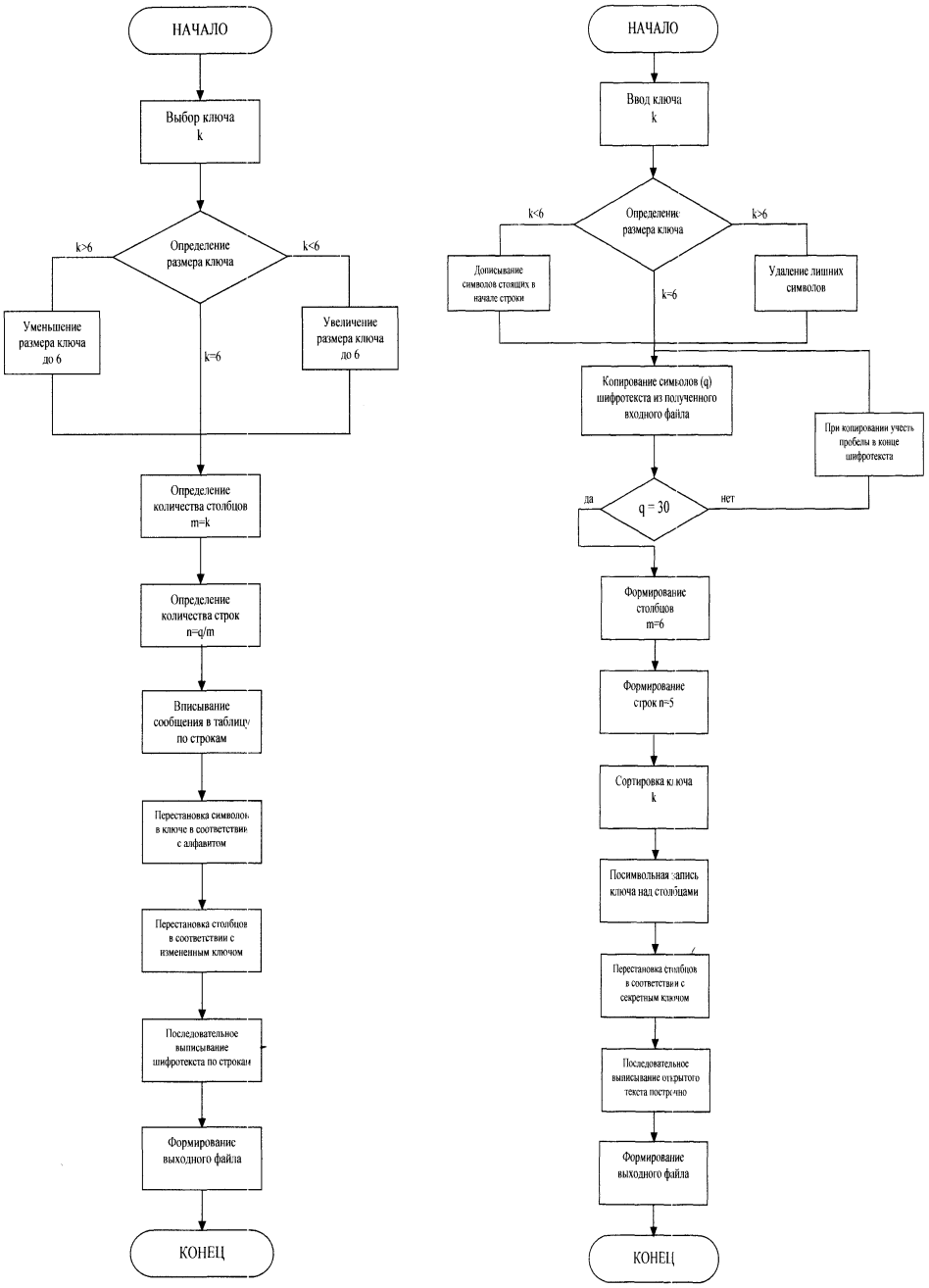

Рисунок. Алгоритм шифрования и алгоритм дешифрования

Программа разработана в соавторстве со студентами, обучающимися по специальности «Организация и технология защиты информации» в рамках НИРС.